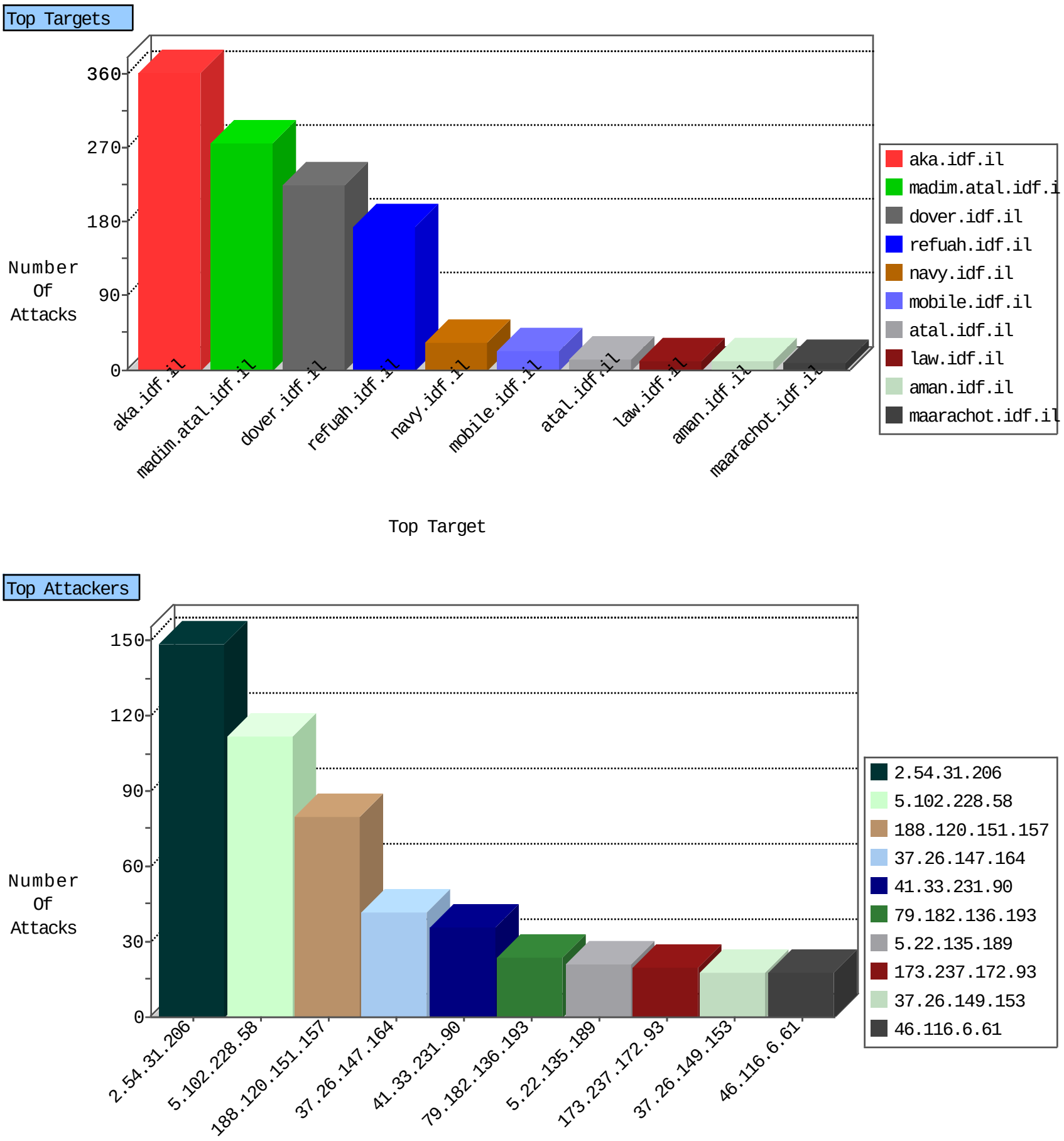
02-10-2016-21:04:02 to 02-10-2016-22:04:02

IDF Under Attack Daily Report



02-10-2016-21:04:02 to 02-10-2016-22:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
74.91.28.58	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1
173.195.0.21	United States	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
74.91.28.59	United States	147.237.76.86	navy.idf.il	block-sp-traf1	drop	1
173.195.0.22	United States	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
142.54.169.164	United States	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
173.195.0.23	United States	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
142.54.169.164	United States	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1

02-10-2016-21:04:02 to 02-10-2016-22:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
155.94.254.143	United States	147.237.77.205	prisha.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
176.86.179.149	Spain	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

02-10-2016-21:04:02 to 02-10-2016-22:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	5
66.249.64.153	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
37.123.100.26	147.237.0.33	Turkey	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.56.46.138	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.3.144.69	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
128.199.61.48	147.237.72.156	Singapore	aman.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
115.124.64.250	147.237.76.86	Indonesia	navy.idf.il	ET SCAN NMAP -f -sS	1
89.138.167.13	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.182.159.29	147.237.0.16	Hungary	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
80.178.184.19	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
139.170.164.9	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
115.124.64.250	147.237.76.86	Indonesia	navy.idf.il	ET SCAN NMAP -sS window 2048	1
94.159.143.62	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.3.84	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.182.159.29	147.237.0.15	Hungary	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
74.4.215.84	147.237.76.30	United States	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

02-10-2016-21:04:02 to 02-10-2016-22:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.102.228.58	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	111
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
5.22.135.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
37.26.147.164	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
173.237.172.93	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	19
46.116.6.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
109.253.156.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
37.26.147.164	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	17
2.54.156.113	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
37.26.149.153	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
79.182.136.193	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.85	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
108.61.211.155	Germany	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.92	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.130.95	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.215.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.18.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.90.167.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.29.9	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
66.249.78.5	United States	147.237.0.19	madim.atal.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.60.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.191.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
172.245.10.186	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
109.253.129.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.128.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.92	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.183.48.38	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.11.12	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.182.136.193	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
37.46.39.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
37.46.39.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.147.164	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.65.102.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.76.105.207	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
188.143.232.15	Russian Federation	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.12.155.88	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.6.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.140.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.136.193	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.169.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.108.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.129.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.161.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.168.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.116.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-10-2016-21:04:02 to 02-10-2016-22:04:02

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.202.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-10-2016-21:04:02 to 02-10-2016-22:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.31.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	88
2.54.31.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	61
188.120.151.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
188.120.151.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	23
46.19.85.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
109.253.156.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
188.143.232.15	Russian Federation	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 188.143.232.15	Block	3
2.54.27.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.183.9.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.178.157.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.250.193.214	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 85.250.193.214 (Unknown SSL Session)	None	2
2.52.11.12	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
94.159.143.62	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catld in www.aka.idf.il/main/sachar/faq.aspx	None	1
85.65.202.64	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	1
109.253.195.14	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 109.253.195.14	None	1
109.66.149.48	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 109.66.149.48	Block	1
37.26.147.164	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
217.194.199.73	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$87 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
87.68.66.249	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1
80.246.133.45	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
109.66.149.48	Israel	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	1
94.178.207.163	Ukraine	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
85.250.35.18	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCity in madim.atal.idf.il/1088-he/meretz.aspx	Block	1
192.116.162.182	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
128.194.135.73	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
79.176.168.197	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
109.66.149.48	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
91.211.192.161	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation FileName in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
80.246.136.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
46.117.213.82	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.66.149.48	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	Block	1
94.178.207.163	Ukraine	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
142.54.160.211	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.1916wh.com/	Block	1
79.178.161.168	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1
109.66.149.48	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
37.142.156.140	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$1 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
91.211.192.161	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
188.143.232.15	Russian Federation	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 188.143.232.15	Block	1
84.108.136.101	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/×¢×˜×?×“	Block	1
46.120.166.87	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$6 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
109.65.21.131	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.58.110.55	Denmark	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
208.115.113.82	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	1
109.66.149.48	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
94.159.143.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/default	Block	1

02-10-2016-21:04:02 to 02-10-2016-22:04:02